

United States Courts
Southern District of Texas
FILED

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

MAR 19 2008

Michael N. Milby, Clerk of Court

IN THE MATTER OF THE
APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN
ORDER: (1) AUTHORIZING THE
INSTALLATION AND USE
OF A PEN REGISTER AND TRAP
AND TRACE DEVICE, AND
(2) AUTHORIZING RELEASE
OF SUBSCRIBER AND OTHER
INFORMATION

§
§
§
§
§
§
§
§
§
§

Magistrate Case No.

H-08-218M

UN-SEALED PER

Ucdar

dated 7/10/09

(UNDER SEAL)

APPLICATION

A. INTRODUCTION

Stuart Burns an Assistant United States Attorney for the Southern District of Texas,
hereby applies to the Court for an Order:

1. Pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing the installation and use of a pen register and trap and trace device¹ on the following telephone, a mobile telephone, with International Mobile Subscriber Identifier (IMSI) 316010115055640, and Urban Fleet Mobile Identifier (UFMI) 62*310572*1 (hereinafter the “**Target Device**”), subscribed to by unknown subscriber and believed to be used by First Name Unknown, (FNU) Last Name Unknown (LNU) a.k.a. Main Man a.k.a. Jack, a.k.a. Chuck, a.k.a. Alphabet, a.k.a. J.

2. Pursuant to 18 U.S.C. §§ 2703(c), 2703(d), 3122, and 3123 and 47 U.S.C. § 1002, directing the **Target Device’s** service provider (including any internet service provider or other

¹ A “pen register” is a “device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication ...” 18 U.S.C. § 3127(3). A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number” or other identifiers “reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information not include the contents of any communication.” 18 U.S.C. § 3127(4).

electronic communications provider providing voice-over IP telephony [VoIP]),² and any and all other telecommunication providers, persons, or entities providing wire or electronic communications service in the United States whose assistance may facilitate the execution of the Order, to disclose or provide, upon oral or written demand by agents of the Federal Bureau of Investigation and Immigration and Customs Enforcement (hereinafter the “**Investigative Agency**”),

a. For the **Target Device**, records or other information pertaining to subscriber(s) or customer(s), including historical cell site information³ and call detail records⁴ (including in two-way radio feature mode) for the sixty (60) days prior to the date the Order is signed by the Court (but not including the contents of communications).

b. For the **Target Device**, after receipt and storage,⁵ records or other information pertaining to subscriber(s) or customer(s), including the means and source of payment for the service and cell site information, provided to the United States on a continuous

² VoIP is essentially a type of hardware and software that allows people to use the internet as a transmission medium for telephone calls. In general, this means sending voice information in the form of digital packets of information rather than sending it through the traditional public switch telephone network.

³ A cell phone must send a radio signal to an antenna tower which, in turn, is connected to the provider's network. The area covered by the tower varies depending on the population density of the area. This area is often divided into thirds--120 degree sectors. “Cell site information” as used in this application refers to the antenna tower and sector to which the cell phone sends its signal. This includes the physical location and/or address of the cellular tower and identification of the particular sector of the tower receiving the signal.

⁴ “Call detail records” are similar to toll records (i.e. historical telephone records of telephone activity, usually listing outgoing calls and date, time, and duration of each call), which are made and retained in the ordinary course of business. However, “call detail records” is the term used when referring to toll records of mobile telephones rather than hardline telephones. Unlike toll records, however, call detail records also include a record of incoming calls and the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state.

⁵

“After receipt and storage” is intended to ensure that the information authorized under these paragraphs is information that is first captured and recorded by the provider before being sent to the Investigative Agency.

basis for (a) the origination of a call from the **Target Device** or the answer of a call to the **Target Device**, (b) the termination of the call and (c) if reasonably available, during the progress of the call, but not including the contents of the communications.

c. After receipt and storage, the following subscriber records and other information for all published, non-published, or unlisted dialing, routing, addressing, or signaling information captured by the pen register and trap and trace device on the **Target Device**:

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;
- (F) date of birth;
- (G) social security number;
- (H) driver's license (state and number);
- (I) contact names and numbers, and
- (J) employment information.

d. Any and all changes (including additions, deletions, and transfers) in service regarding the **Target Device**, including telephone numbers (including IMSIs and UFMIs) and subscriber information (published, non-published, listed, or unlisted) associated with these service changes.

B. CERTIFICATION FOR A PEN REGISTER AND A TRAP AND TRACE DEVICE PURSUANT TO 18 U.S.C. §§ 3122 AND 3123

In support of this application, I state the following:

1. I am an “attorney for the Government” as defined in Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure, and therefore, pursuant to 18 U.S.C. § 3122, may apply for an order authorizing the installation and use of pen registers and trap and trace devices.

2. I certify that the information likely to be obtained from the pen register and trap and trace device on the **Target Device** is relevant to an ongoing criminal investigation being conducted by the **Investigative Agency** in connection with possible violations of federal criminal statutes, including 21 U.S.C. §§ 841(a)(1) and 846 by FNU LNU a.k.a Main Man, a.k.a. Jack, a.k.a. Chuck, a.k.a. Alphabet, a.k.a. J and others.

3. In accordance with 18 U.S.C. § 3121(c), Applicant has informed the **Investigative Agency** that it shall use technology reasonably available to it to restrict the recording or decoding of electronic or other impulses to the dialing, routing, and addressing and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communication.

4. Therefore, based upon the above Certification, and pursuant to 18 U.S.C. §§ 3122 and 3123, I request that the Court issue an order authorizing:

a. The **Investigative Agency** to install, or cause the provider to install, and use, a pen register device(s) anywhere in the United States to record or decode dialing, routing, addressing, or signaling information transmitted⁶ from the **Target Device**, to record the date and time of such dialings or transmissions, and to record the length of time the telephone receiver in

⁶ Including dialing, routing, addressing, or signaling information transmitted over the communication service provider’s network by a two-way radio feature (including, but not limited to, Nextel’s “Direct Connect/Direct Dispatch,” Verizon Wireless’ “Push to Talk,” or Sprint’s “ReadyLink”). This two-way radio feature, like a walkie-talkie, provides communication between similarly equipped mobile phones by pressing a button on the telephone. As mentioned, information transmitted by the two-way radio feature will not disclose content of the call.

question is “off the hook” or connected for incoming or outgoing calls, for a period of sixty (60) days from the date the order is signed by the Court.

b. The **Investigative Agency** to install, or cause the provider to install, and use, a trap and trace device(s) on the **Target Device** anywhere in the United States to capture and record the incoming electronic or other impulses which identify the originating numbers or other dialing, routing, addressing, or signaling information⁷ reasonably likely to identify the source of a wire or electronic communication and to record the date, time, and duration of calls created by such incoming impulses, for a period of sixty (60) days from the date the Order is signed by the Court.

c. That, pursuant to 18 U.S.C. § 3123(b)(1)(c), the requested installation and use of a pen register as well as trap and trace device permit the use of each not only on the **Target Device**, but also on any changed telephone number(s) (PTN[s]) subsequently assigned to an instrument bearing the same ESN, IMSI, IMEI, UFMI, or SIM as the **Target Device**, or any changed ESN, IMSI, IMEI, UFMI and/or SIM subsequently assigned to the same PTN as the **Target Device**, and any additional changed MIN, ESN, IMSI, IMEI, UFMI and/or SIM, whether the changes occur consecutively or simultaneously, listed to the same subscriber or account number as the **Target Device** within the 60-day period authorized by the Order.

5. I further request, pursuant to 18 U.S.C. §§ 3123(a)(1) and 3123(b)(2), that the Order direct that the furnishing of information, facilities, and technical assistance necessary to accomplish the installation and operation of the pen register and trap and trace device by the

⁷ Including dialing, routing, addressing, or signaling information transmitted over the communication service provider’s network by a two-way radio feature (including, but not limited to, Nextel’s “Direct Connect/Direct Dispatch,” Verizon Wireless’ “Push to Talk,” or Sprint’s “ReadyLink”). As mentioned, information transmitted by the two-way radio feature will not disclose content of the call.

Target Device's service provider (including any internet service provider or other electronic communications provider providing VoIP), and any and all other telecommunication providers,⁸ persons, or entities providing wire or electronic communications service in the United States whose assistance may facilitate the execution of the Order (hereinafter, collectively, the "**Target Device's Service Provider[s]**"), occur unobtrusively and with a minimum of interference with the services that are accorded the persons with respect to whom the installation and use is to take place, with reasonably compensation to be paid by the **Investigative Agency** for reasonable expenses directly incurred in providing such information, facilities, and assistance.

6. I further request that the Order direct the **Target Device's Service Provider(s)** furnish the results of the pen register and trap and trace devices to Special Agents of the **Investigative Agency** as soon as practicable, on a continuing basis, twenty-four (24) hours a day for the duration of the order.

C. SPECIFIC AND ARTICULABLE FACTS ESTABLISHING REASONABLE GROUNDS TO BELIEVE THAT SUBSCRIBER RECORDS ARE RELEVANT AND MATERIAL TO AN ONGOING CRIMINAL INVESTIGATION PURSUANT TO 18 U.S.C. § 2703

1. 18 U.S.C. § 2703(d) provides that a court may issue an order authorizing disclosure of a record or other information pertaining to a telephone subscriber or customer (not including the contents of communications) when a United States agency provides the Court with "[S]pecific and articulable facts showing that there are reasonable grounds to believe that ... the

⁸ The reference to "any and all other telecommunication providers" is necessary so that the Court order is still effective in the event that the **Target Device** is transferred to another carrier pursuant to "Local Number Portability" ("LNP"). LNP allows a telephone user to change his telephone company but still keep the same telephone number. However, to transfer (i.e. "port") a telephone number pursuant to LNP, the subscriber information must remain the same. Thus, this reference applies if the **Target Device** is transferred (i.e. "ported") to another telephone carrier, but the telephone number and subscriber information remain the same.

records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

The statute, by its own language, precludes holding the United States to a higher standard of proof, such as probable cause. See Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414 § 207(2), reprinted in 1992 U.S. Code Cong. & Admin. News 4292. The House Report reflected that “[t]his section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant.” See H.R. Rep. No. 103-827, at 31-32 (1994), reprinted in 1994 U.S.C.A.A.N. 3489, 3511-12.

2. For the purposes of obtaining a court order for disclosure as described in 18 U.S.C. §§ 2703(c)(1)(B) and 2703(c)(2), and in order to satisfy the requirements of 18 U.S.C. § 2703(d), Applicant, based on discussions with Special Agent (SA) Peter Hanna, hereby sets forth the following specific and articulable facts showing that there are reasonable grounds to believe that the records and other information identifying subscribers (but not including the contents of communications) for telephone numbers identified through the pen register and trap and trace device on the **Target Device**, cell site information regarding the **Target Device**, subscriber information associated with any service changes regarding the **Target Device**, and the records or other information pertaining to subscribers (but not including the contents of communications) for the **Target Device** will be relevant and material to an ongoing criminal investigation:

a. An investigation initiated by the Federal Bureau of Investigation (FBI) has determined, by the monitoring of court ordered wire interceptions, that FNU LNU a.k.a. Main Man, a.k.a. Jack, a.k.a. Chuck, a.k.a. Alphabet, a.k.a. J has used the **Target Device** to communicate with Kevin Gobert, a known drug trafficker, on multiple occasions, from multiple

locations in the United States for the purpose of discussing the sale of and distribution of controlled substances. Further analysis of specific calls to Kevin Gobert from the **Target Device** has linked FNU LNU a.k.a. Main Man, a.k.a. Jack, a.k.a. Chuck, a.k.a. Alphabet, a.k.a. J to approximately 1200 pounds of marijuana seized from a vehicle and a residence located at 5632 Hammond Dr, Narcross, Georgia 30071 on February 19, 2008.

b. In SA Peter Hanna's experience, information identifying the subscribers for numbers captured by a pen register and trap and trace device, and subscriber information associated with service changes, has yielded information that is relevant and material to narcotics trafficking investigations. Such information includes leads relating to:

- (A) the names of suspected suppliers, customers, and other individuals who assist in the distribution of narcotics;
- (B) the location of "stash" houses where narcotics are stored;
- (C) the identity of transportation sources used by the drug traffickers;
- (D) the locations of money transfer businesses used by members of the operation to launder proceeds of drug trafficking activities or through which money is exchanged with coconspirators;
- (E) the geographic breadth of the suspected drug trafficking cell; and
- (F) the identities of potential organizers, leaders, managers, or supervisors of the suspected trafficking cell by examining the calling patterns revealed by the toll data.

SA Peter Hanna has advised Applicant that, based upon his training and experience, one way to identify coconspirators is to evaluate the pattern of calls made to and from the **Target Device** – and to obtain information identifying subscribers for these calls – and then conduct an

investigation concerning those individuals. Based upon subscriber information, SA Peter Hanna may then direct, where appropriate, other investigators to conduct surveillance at these individuals' addresses and determine if criminal activity was occurring there, which in turn could yield potential names of coconspirators and potential narcotics storage locations used by the organization.

c. Obtaining the subscriber name, address, date of birth, social security number, driver's license information, contact names and numbers, employment information; and method of payment is critical to accurately identifying such subscribers because, among other things:

- (A) if the subscriber name is a common one and/or the subscriber address is not current, it can be difficult to accurately identify the subscriber without a date of birth, driver's license, or social security number, especially in an area with a population as the Southern District of Texas;
- (B) if the subscriber name and address is fictitious, which frequently is the case when criminals purchase telephones, all or part of the remaining identification information may be truthful and help identify the subscriber or lead to identifying other coconspirators; and
- (C) by accurately identifying subscribers using the above-requested information, agents can eliminate innocent individuals as targets.

d. The investigating agents have further advised me that the general geographic location of the **Target Device** derived from cell site information used by the **Target Device** can be used to corroborate the observations of surveillance agents. More specifically, surveillance agents can compare observations of the user of the **Target Device** with cell site information in order to verify the identification and proximate location of the user of the **Target Device**.

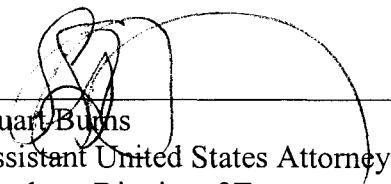
3. Accordingly, based upon the above proffer, and pursuant to 18 U.S.C. §§ 2703(c)(1)(B), 2703(d), 3122, and 3123, because there are reasonable grounds to believe that such information is relevant and material to the ongoing investigation, I further request that the Court issue an Order requiring the **Target Device's Service Provider(s)** disclose, or provide upon oral or written request by Special Agents of the **Investigative Agency**, the information set forth above in Section A2.

D. REQUEST THAT THE ORDER PRECLUDE NOTICE AND THAT THE APPLICATION AND ORDER BE FILED UNDER SEAL

1. Based upon the information provided in this application, I believe disclosure of the requested court Order may result in flight from potential prosecution or the destruction of or tampering with evidence, or may otherwise seriously jeopardize the investigation. Moreover, the exact nature of the United States "pen register" device and its configuration is classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations, and/or future use of the technique. Therefore, pursuant to 18 U.S.C. §§ 2705(b) and 3123(d), I request that this application and Order be SEALED, that the identity of any targets of the investigation may be redacted from any copy of the order served on any service provider or other person, and that the Court direct the **Target Device's Service Provider(s)** not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of the Order, in full or redacted form, of the pen register or trap and trace devices, or of this investigation, to the listed subscriber(s) for the **Target Device**, the occupant of said premises, the subscribers of the incoming calls to or outgoing calls from the **Target Device**, or

to any other person the listed subscriber(s) for the **Target Device**, or to any other person until otherwise ordered by this Court.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on 03/17/2008, at Houston, Texas.



Stuart Burns
Assistant United States Attorney
Southern District of Texas
713-567-9580